(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
27 octobre 2005 (27.10.2005)

PCT

(10) Numéro de publication internationale
WO 2005/101726 A1

(51) Classification internationale des brevets[7] : H04L 9/32

(21) Numéro de la demande internationale :
PCT/FR2005/000528

(22) Date de dépôt international : 4 mars 2005 (04.03.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0402674 16 mars 2004 (16.03.2004) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **CHARLES, Olivier** [FR/FR]; 104, rue Raymond Losserand, F-75014 Paris (FR). **ARDITTI, David** [FR/FR]; 46 ter, rue Paul Vaillant-Coutirier, F-92140 Clamart (FR). **NGUYEN NGOC, Sébastien** [FR/FR]; 60-62, rue Gabriel Péri, F-92320 Chatillon (FR). **BARITAUD, Thierry** [FR/FR]; 16, avenue Dubonnet, F-92400 Courbevoie (FR).

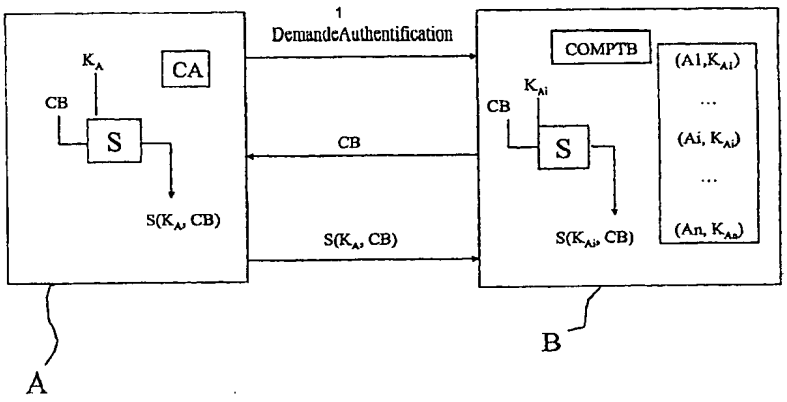
(74) Mandataires : **BENTZ, Jean-Paul** etc.; Novagraff Technologies, 122, rue Edouard Vaillant, F-92593 Levallois-Perret (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,

*[Suite sur la page suivante]*

(54) Title: ANONYMOUS AUTHENTICATION METHOD

(54) Titre : PROCEDE D'AUTHENTIFICATION ANONYME




1 ... AUTHENTICATION REQUEST

(57) **Abstract:** The invention relates to a method for the authentication of a client entity (A) by an authentication entity (B) comprising several secret keys ($K_{Ai}$) which are each associated with a client entity (Ai) to be identified. The inventive method comprises the following steps consisting in: sending an authentication counter value (CB) from the authentication entity (B) to the client entity (A) following an authentication request; at the client entity end, verifying that the counter value received is strictly greater than a counter value (CA) stored by the client entity; at the client entity end, calculating a counter signature (S(K<SB>A</SB>, CB)) and transmitting same to the authentication entity; updating the counter value (CA) stored by the client entity with the authentication counter value (CB); at the authentication entity end (B), looking for a client entity (Ai) to be identified, for which the corresponding counter signature ($S(K_{Ai}, CB)$) is consistent with the received counter signature (S(K<SB>A</SB>, CB)); and increasing the authentication counter (COMPTB).

(57) **Abrégé :** L'invention concerne un procédé d'authentification d'une entité cliente (A) par une entité d'authentification (B) comprenant plusieurs clés secrètes ($K_{Ai}$) associée chacune à une entité cliente (Ai) à identifier, consistant à -envoyer une valeur de compteur d'authentification

*[Suite sur la page suivante]*

WO 2005/101726 A1

CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**

— *avec rapport de recherche internationale*

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

(CB) de l'entité d'authentification (B) vers l'entité cliente (A) suite à une demande d'authentification; -vérifier, côté entité cliente, que la valeur de compteur reçue est strictement supérieure à une valeur de compteur (CA) mémorisée par l'entité cliente; -calculer, côté entité cliente, une signature du compteur ($S(K_A, CB)$) et la transmettre à l'entité d'authentification; -mettre à jour la valeur de compteur (CA) mémorisée par l'entité cliente avec ladite valeur de compteur d'authentification (CB); -rechercher, côté entité d'authentification (B), une entité cliente (Ai) à identifier pour laquelle la signature de compteur correspondante ($S(K_{Ai}, CB)$) est cohérente avec la signature de compteur reçue ($S(K_A, CB)$); -faire croître le compteur d'authentification (COMPTB).